

**IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSE
NASHVILLE DIVISION**

APEX PHYSICAL REHABILITATION &
WELLNESS PLLC, *individually and on
behalf of all others similarly situated,*

Plaintiff,

v.

CHANGE HEALTHCARE INC., a
Delaware corporation, UNITEDHEALTH
GROUP INCORPORATED, a Delaware
corporation, UNITEDHEALTHCARE,
INC., a Delaware Corporation, and
OPTUM, INC., a Delaware Corporation,

Defendants.

CASE NO.: _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Table of Contents

SUMMARY OF THE CASE.....	1
JURISDICTION AND VENUE	5
PARTIES	6
Plaintiff, Apex Physical Rehabilitation & Wellness PLLC	6
Defendant, Change Healthcare Inc.....	7
Defendants, UnitedHealth, UnitedHealthcare, and Optum	8
REQUIREMENTS AND STANDARDS GOVERNING CREATION, COLLECTION, MAINTENANCE, AND USE OF PRIVATE INFORMATION	10
A. Industry Standards	11
B. The Health Insurance Portability and Accountability Act (HIPAA)	15
C. The Federal Trade Commission Act (FTCA)	17
FACTUAL ALLEGATIONS	19
A. Change’s Business	20
B. The Cyberattack	24
C. The Cyberattack on Change Harmed the Class by Disrupting Services Nationwide	27
D. The Cyberattack was a Foreseeable Risk.....	32
E. Defendants Failed to Comply with Requirements and Standards	41
CLASS ALLEGATIONS	43
CAUSES OF ACTION	48
COUNT ONE Negligence (<i>On Behalf of Plaintiff and the Classes</i>)	48
COUNT TWO Negligent Undertaking (<i>On Behalf of Plaintiff and the Classes</i>)	51
COUNT THREE Negligent Failure to Warn (<i>On Behalf of Plaintiff and the Classes</i>)	52
PRAYER FOR RELIEF	53
JURY TRIAL DEMANDED	55

CLASS ACTION COMPLAINT

Plaintiff, Apex Physical Rehabilitation & Wellness PLLC, individually and on behalf of the Class defined herein of similarly situated healthcare providers (“Class Members”), alleges the following against Defendants Change Healthcare Inc. (“Change”), UnitedHealth Group Incorporated (“UnitedHealth”), UnitedHealthcare, Inc. (“UnitedHealthcare”), and Optum, Inc. (“Optum”) (collectively, “Defendants”) based upon corporate knowledge with respect to itself and on information and belief as to all other matters:

SUMMARY OF THE CASE

1. Defendants were at a heightened risk of—and an obvious target for—a cyberattack. This action arises from Defendants’ failure to secure and safeguard their information systems from a massive foreseeable cyberattack that impacted Plaintiff’s and Class Members’ business operations.

2. Defendant Change—a unit of UnitedHealth’s Optum subsidiary—is a “health technology giant” that provides revenue and payment cycle management services that lie at the heart of the U.S. healthcare system. Change’s services connect payers, providers, pharmacies, and patients. The services are critical to providing healthcare throughout the country.

3. Change is known to be the largest clearinghouse for insurance billing and payments in the United States, processing approximately 50% of the nation’s medical claims for approximately 900,000 physicians, 33,000 pharmacies, 5,500 hospitals, and 600 laboratories across the U.S. healthcare system. Change is also regarded as the nation’s largest commercial prescription processor, working with thousands of insurance companies, doctors, pharmacists, and hospitals to help determine patient responsibility for payment.

4. According to Change, its platform is “At the Center of the Healthcare Ecosystem,” it processes 15 billion health care transactions annually—including a range of services that directly affect patient care, such as clinical decision support, eligibility verifications, and pharmacy operations—touches one out of every three U.S. patient records, and its “cloud-based network supports 14 billion clinical, financial, and operational transactions annually.”¹

5. On February 21, 2024, UnitedHealth, the nation’s largest insurer, filed a Form 8-K with the Securities and Exchange Commission disclosing that Change’s systems had been infiltrated and that Private Information in possession of Change had been obtained by an unauthorized party. On or about that date, Change’s systems were accessed by cybercriminals, upon information and belief, due to exploitation of known vulnerabilities in ConnectWise ScreenConnect², identified as CVE-2024-1708 and CVE-2024-1709 (the “Cyberattack”).

6. Following days of public speculation and outrage, Defendants subsequently confirmed that the Cyberattack was a ransomware incident, wherein the cybercriminals accessed Change’s systems and encrypted Change’s (and, upon information and belief, multiple other entities’) data to hold it hostage with the goal of securing a large ransom payment.

¹ Defendants create, collect, transmit, and maintain exorbitant amounts of personal identifiable information (“PII”) and protected health information (“PHI” and, collectively with PII, “Private Information”). The Federal Trade Commission defines “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, but not limited to, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” 17 C.F.R. § 248.201(b)(8). The Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations (collectively, “HIPAA”), generally defines “protected health information” as all individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations.

² StreetConnect is a popular remote desktop software with both on-premise and in-cloud deployments.

7. The Cyberattack, against one of America’s largest healthcare companies was described by the American Hospital Association as “the most serious incident of its kind leveled against a U.S. health care organization.”³

8. As Defendants struggled to bring their systems back online, thousands of healthcare providers throughout the U.S. were locked out of processing payments and, in turn, “struggling to get paid” following the Cyberattack outage. In the meantime, thousands of doctors, hospitals, and other healthcare providers that depend on Change for billing reimbursements remained paralyzed and scrambling without access to Change’s mission-critical services, resulting in overdue payments, interest accumulation, and other financial harm.⁴

9. On or about February 28, 2024, cybercrime group “Blackcat” (also known as “ALPHV,” referred to hereinafter as “ALPHV Blackcat”) claimed credit on its darknet site for the Cyberattack, asserting that it accessed Defendants’ systems and stole millions of sensitive records, including medical insurance and health data on thousands of consumers, healthcare providers, pharmacies, and insurance providers.

³ As the result of the Cyberattack, hospitals, healthcare providers, and pharmacies (including CVS Health and Walgreens) throughout the United States immediately reported their inability to fulfill or process prescriptions through patients’ insurance. By way of example, Tricare, the U.S. military’s health insurance provider for active military personnel, said in a statement that the ongoing Cyberattack was “impacting all military pharmacies worldwide and some retail pharmacies nationally.” Similarly, as a result of the Cyberattack, pharmacies and providers were unable to process drug manufacturer coupons and “co-pay” cards, leaving uninsured or under-insured patients without those critical payment mechanisms they rely on to afford expensive medications and treatments. *Who and what is the hack of UnitedHealth’s tech unit affecting?*, Reuters (March 6, 2024) <https://www.reuters.com/technology/cybersecurity/who-what-is-hack-unitedhealths-tech-unit-affecting-2024-03-06/> (last visited March 7, 2024).

⁴ *Why UnitedHealth, Change Healthcare were targeted by ransomware hackers, and more cybercrime will hit patients, doctors* (March 15, 2024) <https://www.cnn.com/2024/03/15/why-unitedhealth-change-healthcare-were-targets-of-ransomware-hackers.html> (last visited March 18, 2024).

10. The attack was entirely foreseeable and avoidable. On February 19, 2024, ConnectWise had issued a security advisory specifically alerting users of a remote code execution (RCE) flaw—i.e., vulnerabilities CVE-2024-1708 and CVE-2024-1709—that could be leveraged to bypass authentication in ScreenConnect servers, and advised its customers of the need to patch their ScreenConnect servers immediately against the “critical vulnerability”⁵ to prevent RCE attacks. ConnectWise’s alert categorized the vulnerability as a “high” priority, and recommended installing updates as emergency changes or as soon as possible.

11. Indeed, in a Joint Cybersecurity Advisory issued on December 19, 2023, the Federal Bureau of Investigation (“FBI”) and the Cybersecurity & Infrastructure Security Agency (“CISA”) encouraged critical infrastructure organizations, such as Defendants, to implement their various recommendations as set forth in the advisory to reduce the likelihood and impact of inevitable ALPHV Blackcat cyberattack efforts. The FBI and CISA provided various step-by-step technical details associated with the ALPHV Blackcat criminal organization and its attack techniques, and advised organizations of “actions to take today,” which included “prioritize remediation of known exploited vulnerabilities.”⁶

12. Notwithstanding these publicized high-priority, emergent, and critical warnings, Defendants failed to take reasonable, timely and appropriate measures to protect against the foreseeable, catastrophic Cyberattack, including remediation (“patching”) of the known vulnerabilities. As discussed herein in detail, among other failures, Defendants failed to heed credible security warnings; failed to maintain adequate patch management policies and procedures;

⁵ A vulnerability is categorized as “critical” if it could allow the ability to execute remote code or directly impact confidential data or critical systems.

⁶ See FBI and CISA Joint Cybersecurity Advisory (December 19, 2023), available at: [joint-cybersecurity-advisory-tlp-clear-stopransomware-alphv-blackcat-12-19-2023.pdf](https://www.fbi.gov/media/544441) (aha.org).

failed to detect alerts in regard to vulnerabilities affecting its systems; and failed to properly update and patch third-party software, update software regularly, implement third-party patches when issued, and prioritize patches by the severity of the threat.

13. Plaintiff and Class Members are healthcare providers injured as a result of the disruption to their access to Defendants' insurance claims clearinghouse, Defendants' failure to timely and adequately process and pay amounts due and owing to Plaintiff and Class Members for their healthcare services and products, and other financial loss caused by the disruption to Defendants' networks and transactional services.

14. At this time, Plaintiff has not been advised whether its or its patients' confidential information has been compromised. If and when Plaintiff is so advised, it will provide appropriate notices and fully reserves the right to amend to address Defendants' additional liability for any such compromise of its or its patients' confidential information.

15. As a direct and proximate result of Defendants' failures, Plaintiff and the Class Members have suffered and will continue to suffer serious injury.

16. Accordingly, Plaintiff, on behalf of itself and the estimated thousands of similarly situated healthcare providers victimized by the Cyberattack, seeks to hold Defendants responsible for the injuries suffered as the result of their misconduct and failure to act, and demands appropriate monetary, equitable, injunctive, and declaratory relief.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because this is a class action where the amount in controversy exceeds the sum or value of \$5 million, exclusive of interest and costs, there are more than 100 putative

members in the proposed class, and at least one Class Member (e.g., Plaintiff) is a citizen of a state different from any Defendant.

18. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged are part of the same case or controversy.

19. This Court has personal jurisdiction over Defendants. Defendant Change is headquartered and routinely conducts business in the State where this District is located. Each of the Defendants have sufficient minimum contacts in this State, have intentionally availed themselves of this jurisdiction by conducting business in this State, including through marketing and/or selling products and/or services and/or by accepting and processing payments for those products and/or services within this State.

20. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims took place within this District and Defendant Change is headquartered and does business in this Judicial District.

PARTIES

Plaintiff, Apex Physical Rehabilitation & Wellness PLLC

1. Plaintiff Apex Physical Rehabilitation & Wellness PLLC ("Plaintiff") is a Texas professional limited liability company, with a registered office address of 4614 Riverstone Boulevard, Missouri City, Texas.

2. Plaintiff is a physical rehabilitation center, with three locations, one of which is in Houston, Texas.

3. Dr. Amir S. Kazemi, is the founder and chief executive officer of Plaintiff.

4. Like most private healthcare practices, Plaintiff's Houston clinic depends on the timely processing of public and private insurance claims to operate. The majority of Plaintiff's

charges for services provided to its patients are paid for through insurances. The funds Plaintiff receives through insurance payments are necessary to Plaintiff's operation. Those funds are critical, for example, to Plaintiff paying its most essential bills, including payroll, supplies, equipment, rent, and its own insurance.

5. Plaintiff uses the Therabill platform to process its patients' insurance claims and to get paid on those claims.

6. As a direct result of the Cyberattack, approximately 75% of the ordinary payment flow for Plaintiff's Houston clinic stopped. This has placed Plaintiff under financial distress as it depends on its timely payment flow to pay basic operational expenses for the Houston clinic, including payroll, rent, and supplies. Plaintiff is continuing to operate the clinic for now, but Dr. Kazemi is concerned he will have to cut back on services and/or draw on his personal funds if the payment flow is not restored.

7. Plaintiff has come to understand that Therabill was one of many services that used Change Healthcare's platform to timely and accurately process patient insurance claims and provide electronic payments to providers, like Plaintiff, for such claims. As described in more detail below, although Defendants have failed to provide any information directly, Plaintiff is informed and believes that the total breakdown in processing of and payment on Plaintiff's patients' insurance claims is the direct, proximate, and wholly foreseeable result of Defendants' unconscionable failure to secure its systems against the Cyberattack.

Defendant, Change Healthcare Inc.

8. Change is a Delaware corporation, with principal executive offices located at 424 Church Street #1400, Nashville, Tennessee.

9. Change is a subsidiary of Optum, a subsidiary of UnitedHealth, and markets itself as “Part of Optum.”

10. According to Form 10-K filed by UnitedHealth with the Securities Exchange Commission on or about February 24, 2023:

On October 3, 2022, the Company acquired all of the outstanding common shares of [Change] and funded Change’s payoff of its outstanding debt and credit facility for a total of \$13.9 billion in cash. The combination of the Company and Change will connect and simplify the core clinical, administrative and payment processes health care providers and payers depend on to serve patients. Change brings key technologies, connections and advanced clinical decision, administrative and financial support capabilities, enabling better workflow and transactional connectivity across the health care system.

11. As part of the UnitedHealth healthcare empire, Change provides revenue and payment cycle management that connects payers, providers, and patients within the U.S. healthcare system.

Defendants, UnitedHealth, UnitedHealthcare, and Optum

12. UnitedHealth is a Delaware corporation, with principal executive offices located at UnitedHealth Group Center, 9900 Bren Road East, Minnetonka, Minnesota.

13. UnitedHealthcare is a Delaware corporation with principal executive offices located at UnitedHealth Group Center, 9900 Bren Road East, Minnetonka, Minnesota.

14. Optum is a Delaware corporation with principal executive offices located at 13625 Technology Drive, Eden Prairie, Minnesota.

15. UnitedHealth is the parent corporation to UnitedHealthcare, Optum, and Change. Upon information and belief, UnitedHealth operates through four segments, which include UnitedHealthcare and three segments of Optum (i.e., Optum Health, Optum Insight, and OptumRx).

16. Optum has been a subsidiary of UnitedHealth since 2011, and is a parent corporation to Change, having acquired Change in or about October of 2022.

17. In its Form 10-K filed on or about February 24, 2023, UnitedHealth provided the following general overview of its and Optum's services:

UnitedHealth Group Incorporated is a health care and well-being company with a mission to help people live healthier lives and help make the health system work better for everyone. Our two distinct, yet complementary business platforms—Optum and UnitedHealthcare—are working to help build a modern, high-performing health system through improved access, affordability, outcomes and experiences for the individuals and organizations we are privileged to serve.

The ability to analyze complex data and apply deep health care expertise and insights allows us to serve people, care providers, businesses, communities and governments with more innovative products and complete, end-to-end offerings for many of the biggest challenges facing health care today.

Optum combines clinical expertise, technology and data to empower people, partners and providers with the guidance and tools they need to achieve better health. Optum serves the broad health care marketplace, including payers, care providers, employers, governments, life sciences companies and consumers, through its Optum Health, Optum Insight and Optum Rx businesses. These businesses improve overall health system performance by optimizing care quality and delivery, reducing costs and improving consumer and provider experience, leveraging distinctive capabilities in data and analytics, pharmacy care services, health care operations, population health and health care delivery.

UnitedHealthcare offers a full range of health benefits, enabling affordable coverage, simplifying the health care experience and delivering access to high-quality care. UnitedHealthcare Employer & Individual serves employers ranging from sole proprietorships to large, multi-site and national employers, public sector employers and individual consumers. UnitedHealthcare Medicare & Retirement delivers health and well-being benefits for Medicare beneficiaries and retirees. UnitedHealthcare Community & State manages health care benefit programs on behalf of state Medicaid and community programs and their participants.

21. UnitedHealth is regarded as the largest insurer in the United States and, based upon its revenue, the largest company in the U.S. healthcare sector. UnitedHealth maintains several offices within Tennessee including, upon information and belief, offices in Maryville, Kingston, Murfreesboro, and Cordova, Tennessee.

22. UnitedHealthcare markets and sells insurance-related products and services directly to Tennessee consumers, including health insurance coverage plans, short term health insurance plans, individual and family Affordable Care Act marketplace plans, and supplemental, dental, and vision insurance plans within Tennessee. By way of example, on its website,⁷ UnitedHealthcare states, in pertinent part:

Tennessee health insurance plans

You have more insurance options for your health than you think,
Tennessee

If you're self-employed or without insurance from your employer—in other words, you're looking for individual or family health insurance in Tennessee—you might be looking for Affordable Care Act insurance. However, we want to make you aware of the whole range of individual and family insurance products we have available in your state.

23. UnitedHealthcare states further on its website,⁸ in pertinent part:

See why Tennesseans choose UnitedHealthcare

Whatever plan you choose, UnitedHealthcare will help you get the care you need.

- Large variety of network providers
- Low- or no-cost prescription drugs
- Well visits, routine shots
- Dental and vision services
- Transportation to medical appointments.

⁷ <https://www.uhc.com/individuals-families/tennessee>.

⁸ <https://www.uhc.com/communityplan/tennessee>.

24. Optum—via Optum Health, Optum Insight, and Optum Rx—markets and sells insurance-related products and services to Tennessee consumers, including through partnership with TennCare Medicaid plans for pharmacy and other needs, through UnitedHealthcare’s Community Plan, and through benefits maintained for state and higher education employees and local education and government members of the State of Tennessee.⁹

REQUIREMENTS AND STANDARDS GOVERNING CREATION, COLLECTION, MAINTENANCE, AND USE OF PRIVATE INFORMATION

18. Federal and state regulators have established security standards and issued guidelines and recommendations to reduce the risk of cyberattacks, such as data breaches, and the resulting harm to consumers and the healthcare industry. There are a number of state and federal laws, requirements, and industry standards governing the creation, collection, protecting, and use of Private Information.

19. Defendants were or should have been fully aware of the obligations, guidelines, and recommendations with respect to cybersecurity, including their creation, collection, maintenance, protection, and use of Private Information.

A. Industry Standards

20. Cybersecurity experts consistently recognize the healthcare industry as particularly vulnerable to cyberattacks, primarily due to the valuable nature of the Private Information derived through healthcare-related services and products.

⁹ See, e.g., https://www.optumrx.com/oe_tennicare/landing (last visited March 7, 2024) and <https://www.tn.gov/partnersforhealth/other-benefits/emotional-wellbeing-solutions.html> (last visited March 7, 2024).

21. Various cybersecurity industry best practices have been published, are readily available, and should be consulted as a go-to source for an entity instituting, developing, maintaining, or enhancing its cybersecurity standards.

22. These practices include, across all industries encountering Private Information, education and appropriate access restriction for all personnel in regard to proper creation, collection, maintenance, and use of Protected Information; enforcing strong password and similar protections, including multi-factor authentication; applying multi-layer security measures (including firewalls, anti-virus, and anti-malware software); monitoring for suspicious or irregular traffic to servers, credentials used to access servers, activity by known or unknown users, and server requests; implementing encryption¹⁰ to render data unreadable without proper authorization; and regular back up of data.

23. Additional cybersecurity best practices are especially prevalent within the healthcare industry, including, but not limited to, installing appropriate malware detection software, monitoring and limiting network posts, securing web browsers and e-mail systems, configuring network infrastructure (like firewalls, switches, and routers), safeguarding physical security systems, training staff on key cybersecurity aspects, monitoring for vulnerability alerts, and promptly detecting and addressing vulnerability alerts prior to exploitation by cybercriminals.

¹⁰ HHS defined “encryption” as a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (type of formula). If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text. See <https://www.hhs.gov/hipaa/for-professionals/faq/2021/what-is-encryption/index.html> (last visited February 26, 2024).

24. In addition to commonly recognized industry best practices, the National Institute of Standards and Technology (“NIST”) and the Center for Internet Security, Inc. (“CIS”)¹¹ have established standards for reasonable cybersecurity readiness.

25. Recognizing that the national and economic security of the United States is dependent upon the reliable function of critical infrastructure, President Barack Obama issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February of 2013. Executive Order 13636 directed NIST to work with stakeholders to develop a voluntary framework—based on existing standards, guidelines, and practices—for reducing cyber risks to critical infrastructure. Created through collaboration between industry and government, the voluntary framework promotes the protection of critical infrastructure, and provides standards, guidelines, tools, and technologies to protect health information technology systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services.

26. For example, NISTIR 8374, a NIST publication titled “Ransomware Risk Management: A Cybersecurity Framework Profile,” provides basic ransomware tips, including the following:

¹¹ CIS is a community-driven nonprofit responsible for globally recognized best practices for securing IT systems and data, including a prescriptive, prioritized, and simplified set of best practices in cybersecurity (referred to as “CIS Controls”) and consensus-based prescriptive configuration recommendations of global cybersecurity experts (referred to as “CIS Benchmarks”). Per the CI website, the CIS Controls are a general set of recommended practices for securing a wide range of systems and devices, whereas CIS Benchmarks are guidelines for hardening specific operating systems, middleware, software applications, and network devices. The need for secure configurations is referenced throughout the CIS Controls. In fact, CIS Control 4 specifically recommends secure configurations for hardware and software on mobile devices, laptops, workstations, and servers. Both the CIS Controls and the CIS Benchmarks are developed by communities of experts using a consensus-based approach. See <https://www.cisecurity.org/controls/cis-controls-faq> (last visited February 27, 2024).

- Avoid having vulnerabilities in systems that ransomware could exploit.
 - Keep relevant systems fully patched. Run scheduled checks to identify available patches to install these as soon as feasible.
 - Employ zero trust principles in all networked systems. Manage access to all network functions and segment internal networks where practical to prevent malware from proliferating among potential target systems.
 - Inform your technology vendors of your expectations (e.g., in contract language) that they will apply measures that discourage ransomware attacks.
- Quickly detect and stop ransomware attacks and infections.
 - Use malware detection software such as antivirus software at all times. Set it to automatically scan emails and flash drives.
 - Continuously monitor directory services (and other primary user stores) for indicators of compromise or active attack.
 - Block access to untrusted web resources. Use products or services that block access to server names, IP addresses, or ports and protocols that are known to be malicious or suspected to be indicators of malicious system activity.
- Make it harder for ransomware to spread.
 - Use standard user accounts with multi-factor authentication versus accounts with administrative privileges whenever possible.
 - Introduce authentication delays or configure automatic account lockout as a defense against automated attempts to guess passwords.

- Assign and manage credential authorization for all enterprise assets and software, and periodically verify that each account has only the necessary access following the principle of least privilege.
- Store data in an immutable format (so that the database does not automatically overwrite older data when new data is made available).
- Allow external access to internal network resources via secure virtual private network (VPN) connections only.
- Make it easier to recover stored information from a future ransomware event.
 - Make an incident recovery plan. Develop, implement, and regularly exercise an incident recovery plan with defined roles and strategies for decision making. This can be part of a continuity of operations plan. The plan should identify mission-critical and other business-essential services to enable recovery prioritization and business continuity plans for those critical services.
 - Back up data, secure backups, and test restoration. Carefully plan, implement, and test a data backup and restoration strategy—and secure and isolate backups of important data.

B. The Health Insurance Portability and Accountability Act (HIPAA)

27. Change states in its Global Privacy Notice that it “functions as a HIPAA business associate for its HIPAA covered entity payer and provider customers as its primary business function, so Change Healthcare’s creation, collection, use, and disclosure of protected health

information is guided by HIPAA and the terms of a business associate agreement and other contracts.”¹²

28. As a business associate covered under HIPAA (45 C.F.R. § 160.102), Defendants are required to comply with HIPAA Rules, including the Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“*Standards for Privacy of Individually Identifiable Health Information*”), and the Security Rule (“*Security Standards for the Protection of Electronic Protected Health Information*”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.¹³

29. Among numerous obligations imposed by HIPAA,¹⁴ Defendants are required to “comply with the applicable standards, implementation specifications, and requirements,” and to protect against reasonably anticipated threats to the security of sensitive patient health information. Covered entities and business associates must also implement safeguards to ensure the

¹² Change Healthcare Global Privacy Notice, Effective December 2023, available at: https://www.changehealthcare.com/privacynotice?adobe_mc=mcorgid%3d26cd3a665c7d19990a495d73%2540adobeorg%7cts%3d1709006189&adobe_mc=MCORGID%3D26CD3A665C7D19990A495D73%2540AdobeOrg%7CTS%3D1709006561 (last visited February 26, 2024).

¹³ HIPAA’s *Standards for Privacy of Individually Identifiable Health Information* (also known as the “Privacy Rule”) establishes national standards for the protection of medical records and other personal health information. HIPAA’s *Security Standards for the Protection of Electronic Protected Health Information* (also known as the “Security Rule”) establishes national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity. Per the U.S. Department of Health and Human Services’ website, “[t]he Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.” See <https://www.hhs.gov/hipaa/for-professionals/security/index.html>.

¹⁴ Defendants are also subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”). Both HIPAA and HITECH obligate Defendants to follow reasonable security standards, respond to, contain, and mitigate security violations, and protect against disclosure of Private Information. See, e.g., 42 U.S.C. § 17921, 45 C.F.R. § 160.103, 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3)l, 45 C.F.R. § 164.530(f), and 42 U.S.C. § 17902.

confidentiality, integrity, and availability of such information. Safeguards must include physical, technical, and administrative components.

30. The Security Rule requires covered entities, including business associates, to ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and ensure compliance by its workforce.

31. HIPAA also requires Defendants to “review and modify the security measures implemented [...] as needed to continue provision of reasonable and appropriate protection of electronic protected health information” under 45 C.F.R. § 164.306(e), and to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.”¹⁵

C. The Federal Trade Commission Act (FTCA)

32. The Federal Trade Commission (“FTC”) “works to prevent fraudulent, deceptive, and unfair practices that target businesses and consumers.” The Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45, prohibits “unfair or deceptive acts or practices in or affecting commerce.”

¹⁵ 45 C.F.R. § 164.312(a)(1).

33. The FTC has determined that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTCA. The FTC states on its website:¹⁶

This means that companies must not mislead consumers about—among other things—what's happening with their health information. It also means you must ensure your health data practices aren't causing more harm than good. The FTC Act's obligations apply to HIPAA-covered entities and business associates, as well as to companies that collect, use, or share health information that aren't required to comply with HIPAA.

34. Consequently, the FTC has issued numerous guidelines that businesses, such as Defendants, should employ to maintain reasonable cybersecurity practices.¹⁷ For example, the FTC offers guidelines including, but not limited to, the following:

- In managing confidential information, businesses should factor security into the decision making in every department of the business—personnel, sales, accounting, information technology, etc.
- Use an intrusion detection system to expose a breach as soon as it occurs.
- Watch for large amounts of data being transmitted from the system.
- Have a response plan in the event of a breach.

35. With respect to updates and patches to third-party software, the FTC states that outdated software undermines security, the solution being to update software regularly, implement third-party patches as they are issued, prioritize patches by the severity of the threat they are

¹⁶ *Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule*, Federal Trade Commission, <https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach> (last visited February 26, 2024).

¹⁷ *Start with Security: A Guide for Business*, Federal Trade Commission, <https://www.ftc.gov/business-guidance/resources/start-security-guide-business#start> (last visited February 26, 2024).

designed to avert, and use automated tools to track which version of software is running and whether updates are available.

36. Consequently, the FTC strongly encourages businesses to “[p]ut procedures in place to keep your security current and address vulnerabilities that may arise,” including to “[c]heck expert websites (such as www.us-cert.gov) and your software vendors’ websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches to correct problems.”¹⁸ The FTC’s website cites an example case, wherein it charged that a business failed to patch a critical vulnerability because its patch management policies and procedures were inadequate.

37. With respect to security warnings in regard to vulnerabilities, the FTC cautions businesses to heed credible security warnings and move quickly to fix them. The FTC also strongly encourages businesses to “[h]ave an effective process in place to receive and address security vulnerability reports.” Citing an example case, wherein the FTC charged that a business’ alleged delay in responding to warnings meant that the vulnerabilities found their way onto additional devices and across multiple system versions, the FTC warns: “When vulnerabilities come to your attention, listen carefully and then get a move on.”

38. The FTC has brought and routinely brings enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice prohibited by the FTCA. Orders derived from these enforcement actions explicate the measures businesses are required to take to satisfy their cybersecurity obligations.

FACTUAL ALLEGATIONS

¹⁸ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business> (last visited February 26, 2024).

A. Change's Business

39. Change is a “health technology giant” which provides revenue and payment cycle management that connects payers, providers, and patients within the U.S. healthcare system.

40. Change is known to be the largest clearinghouse for insurance billing and payments in the United States, processing approximately 50% of medical claims in the nation for approximately 900,000 physicians, 33,000 pharmacies, 5,500 hospitals, and 600 laboratories across the U.S. healthcare system.¹⁹

41. Change is also regarded as the nation’s largest commercial prescription processor, working with thousands of insurance companies, doctors, pharmacists, and hospitals to help determine patient responsibility for payment.

42. According to Change, its platform is “At the Center of the Healthcare Ecosystem,” it processes 15 billion health care transactions annually—including a range of services that directly affect patient care, such as clinical decision support, eligibility verifications and pharmacy operations—touches one in every three U.S. patient records,²⁰ and its “cloud-based network supports 14 billion clinical, financial, and operational transactions annually.”²¹

43. Change also states on its website:²²

¹⁹ *US health department opens probe into UnitedHealth hack* (Reuters March 13, 2024) <https://www.reuters.com/technology/cybersecurity/hhs-opens-probe-into-hack-unitedhealth-unit-2024-03-13/> (last visited March 18, 2024).

²⁰ AHA Letter to HHS on Implications of Change Healthcare Cyberattack, available at: <https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-healthcare-cyberattack> (last visited February 28, 2024); Sead Fadilpasic, *Change Healthcare hit by major cyberattack—US health tech giant sees website taken offline, login pages unavailable*, <https://www.msn.com/en-us/news/technology/change-healthcare-hit-by-major-cyberattack-us-health-tech-giant-sees-website-taken-offline-login-pages-unavailable/ar-BB1iIJwV> (last visited February 28, 2024).

²¹ <https://www.changehealthcare.com/platform> (last visited February 29, 2024).

²² <https://www.changehealthcare.com/about> (last visited February 26, 2024).

The Change Healthcare Platform provides industry-leading analytics, expansive data, and unparalleled connection and data transfer between providers, payers, and consumers to help improve workflows, increase administrative and financial efficiencies, and improve clinical decisions.

44. Change further states on its website:

We champion innovation through our unified platform to enable a better coordinated, more efficient, and increasingly collaborative healthcare system—one that enables operational efficiencies, optimizes financial performance, and enhances the healthcare experience.

45. With respect to its cybersecurity measures, Change states on its website²³ that it uses “Leading-Edge Technology” to secure customer payment information and accounts. According to Change, it “leverage[s] the latest technology, public and private data sources to fortify our processes and ensure your information is protected.”

46. The Change Healthcare Global Privacy Notice (“Global Privacy Notice”) states in pertinent part:

Privacy matters to Change Healthcare, so we follow a privacy framework that helps us to manage and protect your personal information in the products and services we provide (“Services”) and on our websites (“Sites”). This Global Privacy Notice (“Global Notice”) describes how Change Healthcare collects uses, and shares the personal information from our Sites and Services, the rights and choices that you have about your personal information, and how you can contact us about our privacy practices. Whether you are new to Change Healthcare or a long-time user, please take a moment to review our practices, and if you have any questions contact us through the information in the **How to Contact Us** section below. [emphasis in original]

47. The Global Privacy Notice includes a section titled “Information We Collect From You,” which states, in pertinent part:

²³ <https://support.changehealthcare.com/fraud-prevention> (last visited February 26, 2024).

Change Healthcare collects personal information directly from you, automatically from your devices when you interact directly with our Sites and Services, and from other sources described in the Supplemental Notices. When you interact directly with our Sites and Services, you may not be required to provide us with certain data requested; however, some data is necessary for the purposes described in this Global Notice and if you fail to provide any required data, you may not be able to access our Sites and Services. Where possible, we will allow you to interact with us anonymously or using a pseudonym. However, for most of our functions and activities we usually need your name and contact information.

- **Identifiers:**

- We collect your name, phone number, email address, mailing address, and contact address when you create an account or contact us via the Site and the Services. If you choose to create an account, you will also be asked to create a username and password, and we will assign one or more unique identifiers to your profile. We use this information to provide our Services, respond to your requests, and send information and advertisements to you.
- We collect a unique numerical identifier, assigned to you by a Cookie, automatically when you use the Site and Services in order to identify you, provide our Services, keep you logged in to our Sites, prevent fraud, and provide you with targeted information and offers.

- **Payment information:** We, or a service provider working on our behalf, collect your payment information when you provide it in order to complete a transaction. This information includes your credit card number or bank account number. We use this information to facilitate payments and transactions.
- **Commercial information:** When you engage in transactions with us, we create records of transactions. We may use this information to measure the effectiveness of our Sites and Services and to provide you with targeted information, advertisements, and offers.
- **Visual information:** We may collect visual information such as profile pictures associated with any account you create if you choose to upload one.

- **Professional or employment-related information:** We collect your business contact information when you contact us regarding our Site and Services, or when you interact with us at trade shows. We may also collect your business contact information in the course of providing the Services. We otherwise do not collect your professional or employment-related information.
- **Inferences drawn to create a profile about a consumer reflecting the consumer's preferences or characteristics:** We analyze your actual or likely preferences through a series of computer processes and add our observations to your internal profile. We use this information to gauge and develop our marketing activities, to measure the appeal and effectiveness of our Sites and Services, applications, and tools, and to provide you with targeted information, advertisements, and offers.
- **Browser and device data:** We may collect your device type, operating system and version, IP address, general geographic location as indicated by your IP address, browser type, screen resolution, device manufacturer and model, language, plug-ins, add-ons and the language version of the Site you are visiting.
- **Usage data:** We collect information about the time you spend on the Site, the content you view and features you access, the pages that led or referred you to our Site, language preferences, how you interact with available content, and entered search terms.
- **Your [s]ite [a]ctivity:** We collect any information you choose to include in your messages or responses when interacting with us through our Sites and Services, including via online communities and forums, inquiry forms, our support portal, or our Chatbox messaging service and other messaging services, including any information you provide when you complete a survey administered by us or by a supplier acting on our behalf.
- **Social media:** We collect information that you make available to us on social media platforms (such as by clicking on a social media icon linked from our Sites and Services), including your account ID or username and other information included in your posts. [emphasis in original]

48. The Global Privacy Notice includes a section titled “Information We Collect From Other Sources,” which states, in pertinent part:

We may obtain information about you from other sources such as data brokers, customers, credit reporting agencies, social networks, partners with which we offer co-branded services or engage in joint marketing activities, and publicly available sources such as data in the public domain.

We also may receive information about you from outside suppliers through your online activities on websites and connected devices over time and across websites, devices, apps and other online features and services.

These other sources help us update, expand, and analyze our records; identify new customers; determine you or your organization’s advertising or purchasing preferences; or prevent or detect fraud. We combine such information with information we have collected about you through our Sites and Services. We will treat the combined information in accordance with this Privacy Notice.

49. In light of Change’s representations as to its vast influence and involvement in the U.S. healthcare industry—i.e., its platform is “At the Center of the Healthcare Ecosystem,” processing 15 billion health care transactions annually and touching one out of every three U.S. patient records—and the corresponding amounts of sensitive data it creates, collects, maintains, and uses, Defendants were and continue to be particularly susceptible to a cyberattack.

B. The Cyberattack

50. On or about February 21, 2024, Change experienced a data breach event (i.e., the Cyberattack) through which several terabytes of Private Information in possession of Change and/or Defendants was obtained by an unauthorized party. According to publicly available information, including statements by Defendants, Change’s systems were accessed by

cybercriminals due to exploitation of known ConnectWise ScreenConnect vulnerabilities, identified as CVE-2024-1708 and CVE-2024-1709.

51. According to publicly available information, including statements by Defendants, the Cyberattack was a ransomware data breach attack, wherein the cybercriminals accessed Change's systems and encrypted Change's (and, upon information and belief, multiple other entities') data to hold it hostage with the aim of securing a large ransom payment.

52. Prior to the attack, on February 19, 2024, ConnectWise issued a security advisory specifically alerting users (such as Change) of a remote code execution (RCE) flaw—i.e., vulnerabilities CVE-2024-1708 and CVE-2024-1709—that could be leveraged to bypass authentication²⁴ in ScreenConnect servers, and advised its customers to patch their ScreenConnect servers immediately against the “critical vulnerability” to prevent RCE attacks.

53. ConnectWise's alert categorized the vulnerability as “high” priority, and recommended installing updates as emergency changes or as soon as possible.

54. In a Form 8-K report filed with the Securities Exchange Commission on February 21, 2024, UnitedHealth stated:

Item 1.05. Material Cybersecurity Incidents.

On February 21, 2024, UnitedHealth Group (the “Company”) identified a suspected nation state associated cyber security threat actor had gained access to some of the Change Healthcare information technology systems. Immediately upon detection of this outside threat, the Company proactively isolated the impacted systems from other connecting systems in the interest of protecting our partners and patients, to contain, assess and remediate the incident.

The Company is working diligently to restore those systems and resume normal operations as soon as possible, but cannot estimate

²⁴ Upon information and belief, the exploited flaw allows attackers to bypass authentication and gain RCE on Change's systems through bypassing two-factor authentication via brute force.

the duration or extent of the disruption at this time. The Company has retained leading security experts, is working with law enforcement and notified customers, clients and certain government agencies. At this time, the Company believes the network interruption is specific to Change Healthcare systems, and all other systems across the Company are operational.

During the disruption, certain networks and transactional services may not be accessible. The Company is providing updates on the incident at <https://status.changehealthcare.com/incidents/hqpjz25fn3n7>. Please access that site for further information.

As of the date of this report, the Company has not determined the incident is reasonably likely to materially impact the Company's financial condition or results of operations. [emphasis in original]

55. Change disconnected more than 100 technology services after discovering the attack, causing unprecedented harmful ripple effects throughout the healthcare industry.²⁵

56. On or about February 28, 2024, notorious cybercrime group ALPHV Blackcat claimed on its darknet site responsibility for the attack, claiming it accessed Defendants' systems and stole millions of sensitive records, including medical insurance and health data on thousands of healthcare providers, pharmacies, and insurance providers.

57. One day later, on February 29, 2024, UnitedHealth confirmed the cyberattack, stating: "Change Healthcare can confirm we are experiencing a cyber security issue perpetrated by a cybercrime threat actor who has represented itself to us as ALPHV/Blackcat."²⁶

²⁵ *Medical Providers Fight to Survive After Change Healthcare Hack* (Wall Street Journal March 1, 2024) <https://www.wsj.com/articles/medical-providers-fight-to-survive-after-change-healthcare-hack-328c2e5a?st=xw6912h0q8apmly&reflink> (last visited March 18, 2024).

²⁶ Media sources indicate that, on March 1, 2024, Change paid to ALPHV Blackcat a ransom in response to the attack, in the amount of 350 bitcoins, or approximately \$22 million. *See, e.g., Hacking gang behind pharmacy chaos shuts down again. Will it matter?* (March 6, 2024) <https://www.washingtonpost.com/technology/2024/03/06/ransomware-gang-alphv-shuts-down/> (last visited March 6, 2024).

C. The Cyberattack on Change Harmed the Class by Disrupting Services Nationwide

58. The Cyberattack, against one of America's largest healthcare companies was described by the American Hospital Association as "the most serious incident of its kind leveled against a U.S. health care organization."²⁷

59. As Defendants struggled to bring their systems back online, thousands of healthcare providers throughout the U.S. were locked out of processing payments and, in turn, "struggling to get paid" following the ransomware outage. Thousands of doctors, hospitals, and other healthcare providers that depend on Change for billing reimbursements were paralyzed and scrambling without access to Change's mission-critical services, resulting in unpaid claims, overdue payments, interest accumulation, inability to perform eligibility checks for patients leading to loss of services, increased administrative costs caused by manual processes, negative credit impact, and other financial harm.²⁸

²⁷ As the result of the Cyberattack, hospitals, healthcare providers, and pharmacies (including CVS Health and Walgreens) throughout the United States immediately reported their inability to fulfill or process prescriptions through patients' insurance. By way of example, Tricare, the U.S. military's health insurance provider for active military personnel, said in a statement that the ongoing cyberattack was "impacting all military pharmacies worldwide and some retail pharmacies nationally." Similarly, as a result of the Cyberattack, pharmacies and providers were unable to process drug manufacturer coupons and "co-pay" cards, leaving uninsured or under-insured patients without those critical payment mechanisms they rely on to afford expensive medications and treatments. *Who and what is the hack of UnitedHealth's tech unit affecting?*, Reuters (March 6, 2024) <https://www.reuters.com/technology/cybersecurity/who-what-is-hack-unitedhealths-tech-unit-affecting-2024-03-06/> (last visited March 7, 2024).

²⁸ *Why UnitedHealth, Change Healthcare were targeted by ransomware hackers, and more cybercrime will hit patients, doctors* (March 15, 2024) <https://www.cnn.com/2024/03/15/why-unitedhealth-change-healthcare-were-targets-of-ransomware-hackers.html> (last visited March 18, 2024). According to the proprietor of a Michigan laboratory, over a week after the cyberattack, the lab remained "100 percent down when it comes to billing right now," while six small providers reported to Reuters that "they were unable to process claims and were racking up thousands of dollars in overdue payments." *Healthcare providers hit by frozen payments in ransomware outage*, Reuters (February 29, 2024), available at: <https://www.msn.com/en-us/money/companies/healthcare-providers-hit-by-frozen-payments-in-ransomware-outage/> (last visited February 29, 2024).

60. Following the attack and continuing to date, health systems throughout the United States—including hospitals, physician groups, dental clinics, and pharmacies—also reported that they were unable to fulfill or process prescriptions through patients’ insurance and/or manufacturer coupon/co-pay programs, making prescription medication inaccessible.²⁹

61. In response to the cyberattack, the American Hospital Association stated in a February 26, 2024 letter to HSS,³⁰ in pertinent part:

This unprecedented attack against one of America’s largest health care companies has already imposed significant consequences on hospitals and the communities they serve. Although the full scope of the impact is still unclear, Change Healthcare’s vast nationwide reach suggests that it could be massive. According to Change Healthcare, the company processes 15 billion health care transactions annually and touches 1 in every 3 patient records. These transactions include a range of services that directly affect patient care, including clinical decision support, eligibility verifications and pharmacy operations. All of these have been disrupted over the past several days. Thankfully, Change Healthcare has informed our members that its prior authorization portals are active, but our members are reporting that a substantial portion of their claims still cannot be processed, nor can they complete eligibility checks necessary to determine whether a patient’s insurance covers a prospective treatment.

Change Healthcare’s downed systems also will have an immediate adverse impact on hospitals’ finances and the work they do every day to care for patients and communities. Their interrupted technology controls providers’ ability to process claims for payment, patient billing and patient cost estimation services. Any prolonged disruption of Change Healthcare’s systems will

²⁹ As explained by the operator of seven Kansas pharmacies, the system outage prevented insurance verification and, thus, impacted patient ability to obtain medication. While some patients may have been able to pay cash if the medication is relatively inexpensive, others were unable to obtain more costly treatments for flu or COVID-19. *A Cyberattack on UnitedHealth Unit Disrupts Prescription Drug Orders*, The New York Times (February 26, 2024), available at: <https://www.nytimes.com/2024/02/26/health/cyberattack-prescriptions-united-healthcare.html> (last visited February 29, 2024).

³⁰ AHA Letter to HHS on Implications of Change Healthcare Cyberattack, available at: <https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-healthcare-cyberattack> (last visited February 28, 2024).

negatively impact many hospitals' ability to offer the full set of health care services to their communities. After all, without this critical revenue source, hospitals and health systems may be unable to pay salaries for clinicians and other members of the care team, acquire necessary medicines and supplies, and pay for mission critical contract work in areas such as physical security, dietary and environmental services. In addition, replacing previously electronic processes with manual processes will add considerable administrative costs on providers, as well as divert team members from other tasks. It is particularly concerning that while Change Healthcare's systems remain disconnected, it and its parent entities benefit financially, including by accruing interest on potentially billions of dollars that belong to health care providers.

We appreciate that the resolution to this attack ultimately lies with Change Healthcare and its parent company UnitedHealth Group. We are in communication with their leadership and have asked for certain support, including greater transparency about the nature and scope of the attack, an anticipated timeline for resolution, and temporary access to advanced payments to help providers weather the period while normal claims processing functions are down.

62. The grave concerns raised by the American Hospital Association have materialized and continue to materialize.

63. A spokesman for UnitedHealth estimated that more than 63,000 pharmacies nationwide have been affected by the attack.³¹ Unfortunately for patients who required prescription medication following the cyberattack, they were forced to either forgo critical prescription medication or, if possible, pay out of pocket and without guarantees of reimbursement. Of course, decrease in prescription processing translates to revenue loss for pharmacists and providers.

64. Following the Cyberattack, Tricare, the U.S. military's health insurance provider for active military personnel, said in a statement that the ongoing cyber incident was "impacting

³¹ *WA pharmacies, health systems reel from UnitedHealthcare cyberattack* (February 29, 2024), available at: <https://www.seattletimes.com/seattle-news/health/wa-pharmacies-health-systems-reel-unitedhealthcare-cyberattack/> (last visited February 29, 2024).

all military pharmacies worldwide and some retail pharmacies nationally.” As of February 28, 2024, Tricare’s website stated:³²

Change Healthcare Cyberattack Impact on MHS Pharmacy Operations

A reported cyberattack on the nation’s largest commercial prescription processor, Change Healthcare, continues to affect military clinics and hospitals worldwide. On February 21, Change Healthcare disconnected their systems to protect patient information. This is impacting all military pharmacies worldwide and some retailers nationally.

As of February 28, 2024, military clinics and hospitals will continue to provide prescriptions through manual procedures until this issue is resolved. Military pharmacies will give priority to urgent prescriptions followed by routine prescriptions. Each military hospital and clinic will continue to offer pharmacy operations based on their local manning and resources. Please be patient while pharmacies take longer than usual to safely fill prescription needs.

It is unknown at this time when the issue will be resolved. Beneficiaries are encouraged to contact their military hospital and clinic or retail pharmacy for the latest local updates.

65. Ransomware and cyberattacks can be particularly dangerous within the healthcare industry as they have also been proven to cause immediate harm to patients’ physical safety in addition to lack of prescription or treatment accessibility. By way of examples, according to John Riggi, the national advisor for cybersecurity and risk at the American Hospital Association, “when systems go dark, diagnostic technologies like CT scanners can go offline and ambulances carrying patients are often diverted, which can delay lifesaving care.”³³

³² <https://tricare.mil/GettingCare/VirtualHealth/SecurePatientPortal/PatientPortalOutages> (last visited February 28, 2024).

³³ *Ransomware group Blackcat is behind cyberattack on UnitedHealth division, company says* (February 29, 2024), <https://www.cnn.com/2024/02/29/blackcat-claims-responsibility-for-cyberattack-at-unitedhealth.html> (last visited February 29, 2024).

66. In addition, ransomware and data breaches, such as the instant Cyberattack, have devastating effects on substance abuse and mental health patients and providers across the country. According to a joint statement released by the National Council for Mental Wellbeing and the National Association of Addiction Treatment Providers in response to the Cyberattack, “[i]n the midst of an overdose crisis and an increased demand for mental health treatment, this disruption in vital services has left patients vulnerable to crisis, as behavioral health providers are unable to obtain insurance approval or payment for their services.”³⁴

67. Over three weeks after the Cyberattack took place, with payments to beleaguered healthcare providers throughout the U.S. remaining frozen, and with providers warning that they are struggling to meet payroll, lawmakers pleaded with UnitedHealth to take action.

68. For example, Senator Maggie Hassan (D-N.H.), citing as an example the rural hospitals “hard-hit” by the Change outage and UnitedHealth’s insufficient response, appealed to President Biden for assistance in addressing the healthcare payment crisis. Senator Hassan also forwarded a letter to UnitedHealth and Optum requesting “urgent financial support,” stating in pertinent part: “Due to the Change Healthcare hack, these hospitals have seen nearly all—98 percent—of their claims and cash flow disappear in the last few weeks.”³⁵

69. On or about March 13, 2024, HHS announced that it would investigate the Cyberattack, including the extent of the breach and compliance by Defendants with HIPAA,

³⁴ *Large Scale Cyberattacks Disrupt Essential Substance Abuse and Mental Health Services*, National Association of Addiction Treatment Providers (March 7, 2024) <https://www.naatp.org/resources/news/large-scale-cyberattacks-disrupt-essential-substance-use-and-mental-health-services> (last visited March 7, 2024).

³⁵ *HHS opens probe into UnitedHealth’s cybersecurity as hack fallout continues* (March 13, 2024) <https://www.washingtonpost.com/health/2024/03/13/patient-data-breach-hhs-probe-unitedhealth-change-healthcare/> (last visited March 18, 2024).

“Given the unprecedented magnitude of this cyberattack, and in the best interest of patients and health care providers.”³⁶

70. The Cyberattack had, and continues to have, damaging rippling effects for providers linked to Defendants’ claims-processing and other systems, especially since medical businesses tend to have extremely high costs and typically operate without a lot of cash on hand.³⁷

71. To make matters worse, if and when the Change systems are restored, claims backlog will be extreme.³⁸

72. Healthcare practitioners across the U.S. “have seen cash flow dry up.” According to a survey of 1,000 hospitals conducted by the American Hospital Association, 60% of respondents said the impact to revenue was \$1 million or more per day.³⁹

73. Indeed, the cyberattack has “crippled revenue flow in the healthcare sector,” has been called “‘the most serious incident of its kind’ to strike healthcare, [and] has pushed many medical providers to the brink of closure.”⁴⁰

D. The Cyberattack was a Foreseeable Risk

³⁶ *Id.*

³⁷ *Medical Providers Fight to Survive After Change Healthcare Hack* (Wall Street Journal March 1, 2024) <https://www.wsj.com/articles/medical-providers-fight-to-survive-after-change-healthcare-hack-328c2e5a?st=xw6912h0q8apmly&reflink> (last visited March 18, 2024). As one of many examples, due to the devastating financial impact of the Cyberattack, Equine Healing Collaborative, a California provider with four locations, was owed over \$50,000 in unpaid claims (as of March 1), necessitating that five clinicians be furloughed. *Id.*

³⁸ *Id.*

³⁹ *Change Healthcare Hack: What You Need to Know* (Wall Street Journal March 18, 2024) <https://www.wsj.com/articles/change-healthcare-hack-what-you-need-to-know-45efc28c?st=71s1hpcxdx4qcib&reflink> (last visited March 18, 2024).

⁴⁰ *Id.*

74. Healthcare entities in possession of valuable Private Information are particularly susceptible to cyberattacks. Therefore, as an entity subject to HIPAA and involved in the routine creation, collection, maintenance, and use of Private Information, Defendants were at a heightened risk of—and an obvious target for—a cyberattack.

75. Cybercriminals and data thieves regularly target healthcare organizations because of the highly sensitive (and extremely valuable) information maintained by such entities, including financial information of patients, login credentials, insurance information, medical records and diagnoses, and other private personal information of patients, customers, employees, and providers.

76. In addition, “even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized.”⁴¹

77. Identity theft of healthcare data is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, “medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013,” more than identity thefts involving banking and finance, the government, and the military or education.⁴²

⁴¹ The HIPAA Journal, *Editorial: Why Do Criminals Target Medical Records* (October 14, 2022), <https://www.hipaajournal.com/why-do-criminals-target-medical-records/> (last visited February 27, 2024).

⁴² Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News, February 7, 2014, <https://khn.org/news/rise-of-identity-theft/> (last visited February 28, 2023).

78. Private Information—such as the information created, maintained, and transmitted by Defendants—is a valuable commodity and, consequently, a frequent intentional target to cybercriminals. Thus, the Cyberattack was entirely foreseeable.

79. The value of Private Information is self-evident considering the value of “big data” in corporate America and that consequences of cybercrimes include heavy criminal penalties. The risk-to-reward analysis illustrates, beyond question, that Private Information has considerable market value.

80. Indeed, the U.S. Attorney General confirmed in 2020 that “hackers” target consumers’ sensitive personal information because it “has economic value.”⁴³

81. Numerous sources cite pricing for stolen Private Information. According to one report, a healthcare data record may be valued at up to \$250.00 per record on the black market, compared to \$5.40 for the next highest value record (i.e., a payment card).⁴⁴ According to various other sources, Private Information can be sold at prices ranging from \$40.00 to \$200.00 per record, bank details can be sold at prices ranging from \$50.00 to \$200.00 per record,⁴⁵ and a stolen credit or debit card number can sell for \$5.00 to \$110.00.⁴⁶ In addition, criminals can purchase access to

⁴³ *Attorney General William P. Barr Announces Indictment of Four Members of China’s Military for Hacking into Equifax*, U.S. Dep’t of Justice (February 10, 2020), available at <https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military> (last visited February 27, 2024).

⁴⁴ *Hackers, Breaches, and the Value of Healthcare Data* (February 2, 2022), <https://www.securelink.com/blog/healthcaredata-new-prize-hackers/> (last visited February 27, 2024).

⁴⁵ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends (October 16, 2019), available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-darkweb-how-much-it-costs/> (last visited February 27, 2024).

⁴⁶ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian (December 6, 2017), available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-yourpersonal-information-is-selling-for-on-the-dark-web/> (last visited Jan. 31, 2024).

the entirety of a company's breached database on the dark web,⁴⁷ and would expect a sale price of \$999.00 to \$4,995.00.⁴⁸

82. According to one Reuters report,⁴⁹ derived from an investigation which included interviews with nearly a dozen healthcare executives, cybersecurity investigators, and fraud experts:

- Medical data for sale on underground markets “includes names, birth dates, policy numbers, diagnosis codes and billing information.”
- According to investigating experts, fraudsters commonly use such medical data “to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers.”
- A consumer's medical information is worth ten times more than the consumer's credit card number on the black market.
- Medical identity theft is often not immediately identified, giving cybercriminals years to “milk such credentials.”

83. At all relevant times, Defendants' susceptibility to cyberattack was known and obvious to Defendants. The increased vulnerability of healthcare data to cyberattacks has been a

⁴⁷ See, e.g., *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymousbrowsing/in-the-dark/> (last visited February 27, 2024); *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct.16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-darkweb-how-much-it-costs/> (last visited February 27, 2024).

⁴⁸ *In the Dark*, VPNOverview (2019), available at: <https://vpnoverview.com/privacy/anonymousbrowsing/in-the-dark/> (last visited February 28, 2024).

⁴⁹ Caroline Humer and Jim Finkle, *Your medical record is worth more to hackers than your credit card*, <https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924/> (last visited February 28, 2024).

known industry concern for over a decade. Defendants were on notice of numerous public announcements concerning data breaches affecting the healthcare industry, knew that the Private Information it created, collected, maintained, and used is highly coveted by and a frequent target of cybercriminals, experienced past cyberattacks, and, upon information and belief, were notified directly by the government and other stakeholders of their susceptibility to attack.

84. At all relevant times, Defendants were or should have been aware that the Private Information they created, collected, and stored was an attractive target for malicious actors.

85. At all relevant times, Defendants knew or reasonably should have known of the importance of safeguarding Private Information and the foreseeable consequences that would occur if their data security systems were breached, including, specifically, the significant financial harm that would be imposed on providers in the event of a forced disconnect from Defendants' systems.

86. Knowing that its platform is "At the Center of the Healthcare Ecosystem," Change knew or reasonably should have known that an attack on its information systems would be catastrophic in the event of a forced disconnect, and the healthcare sector in the U.S. would be ground to a halt in the event of a cyberattack.

87. Knowing that its subsidiary's platform is "At the Center of the Healthcare Ecosystem," Optum knew or reasonably should have known that an attack on its and its subsidiary's information systems would be catastrophic in the event of a forced disconnect, and the healthcare sector in the U.S. would be ground to a halt in the event of a cyberattack.

88. As the largest insurer in the United States and the largest company in the U.S. healthcare sector, UnitedHealth knew or reasonably should have known that an attack on its or its

affiliates' information systems would be catastrophic in the event of a forced disconnect, and the healthcare sector in the U.S. would be ground to a halt in the event of a cyberattack.

89. Defendants' failure to maintain the security of its information systems is exacerbated by repeated warnings and alerts directed at implementation of appropriate security systems to protect and secure sensitive data. Indeed, cyberattacks, such as the one experienced by Defendants have become so notorious that the FBI, U.S. Secret Service, and other authorities have issued warnings to potential targets so they are aware of, can prepare for and, hopefully, are able to ward off a potential attack.

90. As early as 2011, the FBI had issued warnings regarding the advancement in cybercriminals' abilities to remotely attack systems, particularly those in healthcare, and exploit the systems to obtain Private Information. This warning was not only a prediction of the general escalation of cybercrime, but also was a clear indication to entities such as Defendants of the impending risks associated with the storage and handling of sensitive healthcare data.⁵⁰

91. As early as 2014, in response to a cyberattack on Community Health Systems Inc. and to enable entities within the healthcare industry to take necessary precautions to thwart such attacks, the FBI alerted the healthcare industry that it is an increasingly preferred target of cybercriminals. The FBI's "flash" alert stated,⁵¹ in pertinent part:

The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (PII). These actors have also been seen targeting multiple companies in

⁵⁰ Gordon M. Snow, *Statement before the House Financial Service Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), <https://archives.fbi.gov/archives/news/testimony/cybersecurity-threats-to-the-financial-sector> (last visited February 28, 2024).

⁵¹ Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, Reuters (August 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK2_4U20140820 (last visited February 28, 2024).

the healthcare and medical device industry typically targeting valuable intellectual property, such as medical device and equipment development data.

92. In an October 2, 2019 Public Service Announcement titled “High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations,” the FBI reiterated to the healthcare industry and public that “[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector.”⁵²

93. The American Medical Association has also emphasized the significance of cybersecurity in healthcare, noting it as a technical concern and a vital aspect of patient safety, and highlighting that cyberattacks threaten patient access to care in addition to the privacy and security of patients’ Private Information. According to research conducted by the American Medical Association, as of October 2019, 83% of physicians are part of practices that have been affected by cyberattacks.⁵³

94. On March 10, 2021, the Tenable Security Response Team (SRT) published its analysis of data breaches between January 2020 and October 2020, concluding that the healthcare sector was “by far the most affected industry sector” and that “ransomware is the root cause in a majority of the healthcare breaches analyzed.” According to its root cause analysis of 293 healthcare breaches known to have exposed records between January 2020 and February 2021, the

⁵² *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*, FBI Public Service Announcement, Alert Number I-100219-PSA (October 2, 2019), available at: <https://www.ic3.gov/Media/Y2019/PSA191002> (last visited February 27, 2024).

⁵³ Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, American Medical Association (Oct. 4, 2019), <https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-downclinics-hospitals> (last visited February 27, 2024).

Tenable SRT concluded that “ransomware was by far the most prominent root cause of healthcare breaches, accounting for a whopping 54.95%.”⁵⁴

95. In addition to these industry-specific warnings, trends in cybercrime within the healthcare industry have demonstrated an alarming increase in the frequency and sophistication of attacks. These attacks include, without limitation, attacks on the following entities: American Medical Collection Agency (25 million patients in March 2019), University of Washington Medicine (974,000 patients in December 2018), Florida Orthopedic Institute (640,000 patients in July 2020), Wolverine Solutions Group (600,000 patients in September 2018), Oregon Department of Human Services (645,000 patients in March 2019), Elite Emergency Physicians (550,000 patients in June 2020), Magellan Health (365,000 patients in April 2020), and BJC Health System (286,876 patients in March 2020).

96. Indeed, in an article published by HHS on October 31, 2023, in an effort to bring awareness to Cybersecurity Awareness Month, HHS noted that “[r]ansomware and hacking are the primary cyber-threats in health care.” According to HHS statistics, since 2019 there has been a 239% increase in large breaches reported to HHS’ Office for Civil Rights and a 278% increase in ransomware attacks. Further, in the first ten months of 2023, more than 88 million individuals—one quarter of Americans—had their medical data exposed, a 60% increase from 2022.⁵⁵

⁵⁴ Rody Quinlan, *Healthcare Security: Ransomware Plays a Prominent Role in COVID-19 Era Breaches*, <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches> (last visited February 27, 2024).

⁵⁵ HHS’ Office for Civil Rights, *HHS’ Office for Civil Rights Settles Ransomware Cyber-Attack Investigation* (October 31, 2023) <https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attack-investigation.html> (last visited February 27, 2024).

97. In compiling and analyzing data breach statistics, for a period covering October 2009 through 2023, the HIPAA Journal reported:⁵⁶

Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more records have been reported to the HHS' Office for Civil Rights. Those breaches have resulted in the exposure or impermissible disclosure of 382,262,109 healthcare records. That equates to more than 1.2X the population of the United States. In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day.

98. The continual increase in cyberattacks within the healthcare industry underscored the necessity for Defendants to implement advanced security measures, such as regular security audits.

99. In a Joint Cybersecurity Advisory issued on December 19, 2023, approximately two months prior to the Cyberattack, the FBI and CISA encouraged critical infrastructure organizations such as Defendants to implement their various recommendations set forth in the advisory to reduce the likelihood and impact of ALPHV Blackcat ransomware and data extortion incidents. The FBI and CISA provided various step-by-step technical details associated with the ALPHV Blackcat criminal organization and its attack techniques, and advised organizations of "actions to take today," which included "prioritize remediation of known exploited vulnerabilities."⁵⁷

100. Furthermore, days prior to the December 19 Joint Cybersecurity Advisory, on December 8, 2023, United Healthcare Services Inc. filed a notice of data breach with the Attorney

⁵⁶ The HIPAA Journal, *healthcare Cyberattack Statistics*, <https://www.hipaajournal.com/healthcare-data-breach-statistics/> (last visited February 27, 2024).

⁵⁷ See FBI and CISA Joint Cybersecurity Advisory (December 19, 2023), available at: [joint-cybersecurity-advisory-tlp-clear-stopransomware-alphv-blackcat-12-19-2023.pdf](https://www.fbi.gov/media/584441) (aha.org).

General of Montana after discovering that an unauthorized party accessed an e-mail account of one of its vendors, Equality Health, leading to the exfiltration of sensitive patient information.

101. Based on the foregoing, it is beyond reasonable dispute that Defendants knew or should have known that their electronic records would be targeted by cybercriminals and that Defendants had an obligation and duty to take all reasonable means to protect their information systems from attacks such as the subject Cyberattack.

102. Notwithstanding the common knowledge of, and the prevalence of public announcements and abundance of other publicly available resources with respect to, the imminent and serious threat of cyberattacks within the healthcare industry; notwithstanding the data breach that had recently struck UnitedHealth; and despite its creation, collection, maintenance, and use of Private Information of millions of individuals and entities, Defendants failed to implement reasonable cybersecurity measures. Had Defendants implemented reasonable cybersecurity measures, cybercriminals never could have infiltrated their information systems and the Cyberattack would have been prevented or, at a minimum, of a much smaller scope.

E. Defendants Failed to Comply with Requirements and Standards

103. Defendants failed to implement and comply with industry standards in regard to cybersecurity including, but not limited to, failure to heed credible security warnings; failure to maintain adequate patch management policies and procedures; failure to detect alerts in regard to vulnerabilities affecting its systems; failure to properly update and patch third-party software, update software regularly, implement third-party patches when issued, and prioritize patches by the severity of the threat; failure to properly use automated tools to track which versions of software were running and whether updates were available; and failure to implement appropriate

procedures to keep security current and address vulnerabilities, including to monitor expert websites and software vendors' websites regularly for alerts about new vulnerabilities.

104. Defendants failed to meet the minimum standards of any of the following best practices and frameworks: CIS and NIST publications (including, without limitation, "Ransomware Risk Management: A Cybersecurity Framework Profile"), the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and CIS's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness and response.

105. Defendants violated HIPAA and HITECH. By way of examples, Defendants failed to maintain adequate security practices, systems, and protocols (e.g., Defendants failed to heed credible security warnings, maintain adequate patch management policies and procedures, detect alerts in regard to vulnerabilities affecting their systems, and to properly update and patch third-party software).

106. Defendants failed to comply with the FTCA. By way of examples, Defendants failed to heed credible security warnings; failed to maintain adequate patch management policies and procedures; failed to detect alerts in regard to vulnerabilities affecting its systems; failed to properly update and patch third-party software, update software regularly, implement third-party patches when issued, and prioritize patches by the severity of the threat; failed to properly use automated tools to track which versions of software were running and whether updates were available; and failed to implement appropriate procedures to keep security current and address vulnerabilities, including failure to monitor expert websites and software vendors' websites regularly for alerts about new vulnerabilities.

107. Defendants' acts and failure to act, as set forth above, were willful or reckless or, at the very least, negligent.

CLASS ALLEGATIONS

108. Plaintiff brings this class action individually on behalf of itself and on behalf of all members of the following Class and Subclass (collectively, the "Classes") of similarly situated persons pursuant to Federal Rule of Civil Procedure 23.

109. As described below, this action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of Rule 23(a) and 23(b)(3) (as well as the requirements for certification of one or more issue classes under Rule 23(c)(4)). Accordingly, Plaintiff seeks certification under Federal Rule of Civil Procedure 23 of the following Class and Subclass:

- **Nationwide Class:** All healthcare providers within the United States who have suffered delays in processing claims and revenue cycle services as a result of the Cyberattack.
- **Texas Subclass:** All healthcare providers within Texas who have suffered delays in processing claims and revenue cycle services as a result of the Cyberattack.

110. Excluded from the Classes are (1) Defendants and their affiliates, parents, subsidiaries, officers, agents, and directors, any entity in which Defendants have a controlling interest; (2) all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; (3) those persons who have suffered personal injuries as a result of the facts alleged herein; (4) any and all federal, state, or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsel, and/or subdivisions; and (5) all judges presiding over this matter or assigned to hear any aspect of this litigation, along with judicial clerks and staff, and immediate family members.

111. Plaintiff reserves the right to modify or amend the foregoing Class and Subclass definitions before the Court determines whether certification is appropriate.

112. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure 23 because there is a well-defined community of interest in the litigation and membership in the proposed Classes is readily ascertainable.

113. **Numerosity (Federal Rule of Civil Procedure 23(a)(1)):** A class action is the only available method for the fair and efficient adjudication of this controversy. The members of each Class are so numerous and geographically dispersed that individual joinder of all Class Members is neither practicable nor possible. Plaintiff is informed and believes and, on that basis, alleges that the total number of Class Members is in the thousands. Membership in the Class will be determined by analysis of Defendants' records.

114. **Commonality (Federal Rule of Civil Procedure 23(a)(2) and (b)(3)):** Consistent with Rule 23(a)(2) and with Rule 23(b)(3)'s predominance requirement, Plaintiff and Class Members share a community of interest in that there are numerous common questions and issues of law and fact which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

- a. Whether Defendants owed a duty to Plaintiff and Class Members to safeguard the information systems targeted in the Cyberattack;
- b. Whether Defendants knew, or should have known, of the susceptibility of their information systems to attack;
- c. Whether Defendants were negligent in maintaining, protecting, and securing their information systems;

- d. Whether Defendants were negligent in failing to adequately monitor, audit, and repair the information systems;
- e. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Cyberattack to occur;
- f. Whether Defendants failed to notify Plaintiff and Class Members as soon as practicable and without delay after the Cyberattack was discovered;
- g. Whether Defendants failed to take reasonable and prudent security measures with respect to their information systems;
- h. Whether Defendants' security measures to protect its systems were reasonable in light of known legal requirements;
- i. Whether Defendants failed to comply with applicable laws, regulations, and industry standards related to their information systems;
- j. Whether Defendants failed to comply with their own policies and procedures related to their information systems;
- k. Whether Defendants violated federal statutes including, but not limited to, HIPAA and FTCA;
- l. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to prevent or respond to the Cyberattack;
- m. Whether Defendants knew or should have known that their information systems and monitoring processes were deficient;
- n. Whether Defendants' conduct, including its alleged failure to act, resulted in or was the proximate cause of the Cyberattack; and

- o. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

115. In the alternative, Plaintiff seeks certification under Rule 23(c)(4) with respect to one or more of the above issues or such other issues as may be identified in the future.

116. **Typicality (Federal Rule of Civil Procedure 23(a)(3)):** Plaintiff's claims are typical of the claims of the Classes. As the result of Defendants' common course of conduct in violation of laws and standards, as alleged herein, Plaintiff sustained damages akin to damages sustained by all Class Members, including financial loss caused by Defendants' failure to timely and adequately process and pay amounts due and owing to Plaintiff and Class Members for their medical services, and other harm caused by the disruption to Defendants' networks and transactional services.

117. **Adequacy (Federal Rule of Civil Procedure 23(a)(4)):** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of each of the Classes because Plaintiff is a member of the Classes and is committed to pursuing this matter against Defendants to obtain relief for the Classes. Plaintiff is not subject to any individual defense unique from those conceivably applicable to other Class Members or the Classes in their entirety. Plaintiff anticipates no management difficulties in this litigation. Plaintiff has no conflicts of interest with the Classes. Plaintiff's Counsel is competent and experienced in litigating class actions, including extensive experience in litigation in regard to cyberattacks. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Classes' interests.

118. **Predominance and Superiority (Federal Rule of Civil Procedure 23(b)(3)):** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be

encountered in the management of this class action. Common issues in this litigation predominate over individual issues. The issues discussed above in regard to commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class-action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class Members are relatively small compared to the burden and expense required to individually litigate their respective claims against Defendants, and thus, individual litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by each Class Member would also burden and unreasonably strain the court system, and would result in undue delay. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class-action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

119. **Ascertainability:** The Class and Subclass are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Classes. Defendants have access to names in combination with addresses and/or e-mail addresses of Class Members affected by the Cyberattack.

120. **Injunctive and Declaratory Relief:** This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate concerning the Classes in their entirety. Defendants' policies and practices challenged herein apply to and affect Class Members uniformly. Plaintiff's challenge of these policies and

procedures hinges on Defendants' conduct concerning the Classes in their entirety, not on facts or law applicable only to Plaintiff. Unless a Class-wide injunction is issued, Defendants may continue failing to properly process claims or secure their information systems, and Defendants may continue to act unlawfully, as set forth in this Complaint. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under F.R.C.P. Rule 23(b)(2).

CAUSES OF ACTION

COUNT ONE

Negligence

(On Behalf of Plaintiff and the Classes)

121. Plaintiff restates, re-alleges, and incorporates by reference each and every allegation of the preceding paragraphs of this Complaint as though fully set forth herein.

122. At all times relevant hereto, Defendants owed Plaintiff and Class Members a duty to act with reasonable care to ensure continuity of their Defendants' networks and transactional services, and to ensure that their revenue cycle services would be adequately performed, including by way of timely and accurate claims processing. Defendants assumed this obligation and utilized their information systems in the performance of their services on behalf of Plaintiff and Class Members.

123. In regard to their information systems, practices, and protocols, Defendants knew or should have known of the necessity to, *inter alia*, heed credible security warnings; maintain adequate patch management policies and procedures; detect alerts in regard to vulnerabilities affecting its systems; properly update and patch third-party software, update software regularly, implement third-party patches when issued, and prioritize patches by the severity of the threat;

properly use automated tools to track which versions of software were running and whether updates were available; and implement appropriate procedures to keep security current and address vulnerabilities, including to monitor expert websites and software vendors' websites regularly for alerts about new vulnerabilities.

124. It was reasonably foreseeable to Defendants that Plaintiff and the Class Members would suffer such harms in the event of a cyberattack such as the subject Cyberattack.

125. Defendants owed a duty to Plaintiff and Class Members to provide reasonable security, consistent with industry standards and requirements, and to ensure that their computer systems, networks, and protocols, and the personnel responsible for them, were sufficient.

126. Defendants owed a duty to Plaintiff and Class Members to design, maintain, and test their computer systems, servers, and networks to ensure that their information systems and networks were adequately secured and protected.

127. Defendants owed a duty to Plaintiff and Class Members to create and implement reasonable security systems, networks, practices, and protocols.

128. Defendants owed a duty to Plaintiff and Class Members to implement and maintain processes that would immediately detect a breach of their information systems or networks.

129. Defendants owed a duty to Plaintiff and Class Members to act upon cybersecurity warnings and alerts in a timely fashion.

130. Defendants owed a duty to Plaintiff and Class Members to disclose in timely fashion if their computer systems and data security practices were inadequate in any way, because such vulnerability or inadequacy would be a material fact in the decision to engage in business transactions with Defendants.

131. Plaintiff and the Class Members were foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in failing to heed credible security warnings; failing to maintain adequate patch management policies and procedures; failing to detect alerts in regard to vulnerabilities affecting its systems; failing to properly update and patch third-party software, update software regularly, implement third-party patches when issued, and prioritize patches by the severity of the threat; failing to properly use automated tools to track which versions of software were running and whether updates were available; and failing to implement appropriate procedures to keep security current and address vulnerabilities, including to monitor expert websites and software vendors' websites regularly for alerts about new vulnerabilities.

132. Defendants' failure to abide by their duties was wrongful and negligent in light of the foreseeable risks and known threats.

133. Only Defendants were in the position to ensure that their information systems, networks, practices, and protocols were sufficient.

134. Defendants' duties extended to protecting Plaintiff and the Class Members from the foreseeable risk of foreseeable criminal conduct of third parties, including because Defendants' own actions and omissions exposed Plaintiff and similarly situated parties to the harm flowing from the disruption of routine, timely processing of patients' insurance claims and insurers' payments for services.

135. But for Defendants' breaches of the duties they owed to Plaintiff and the Class Members, Plaintiff and Class Members would not have suffered financial and other harm.

136. There is a close causal connection between Defendants' failures—including, but not limited to failure to adopt, implement, and maintain security measures to protect their

information systems—and the harm suffered by Plaintiff and the Class Members. Defendants’ failure to exercise reasonable care in adopting, implementing, and maintaining appropriate security measures to protect their information systems resulted in loss of Change’s mission-critical services, and was the proximate result of overdue payments, interest accumulation, and other financial harm to Plaintiff and Class Members.

137. As a direct and proximate result of Defendants’ negligence, Plaintiff and the Class Members have suffered and will suffer injury.

COUNT TWO
Negligent Undertaking
(On Behalf of Plaintiff and the Classes)

138. Plaintiff restates, re-alleges, and incorporates by reference each and every allegation of the preceding paragraphs of this Complaint as though fully set forth herein.

139. By agreeing to serve as a claims clearinghouse and payment processor, Defendants undertook to render revenue and payment cycle management services that benefitted Plaintiff and Class Members.

140. In undertaking to provide such services to Plaintiff and Class Members, Defendants knew or should have known of the necessity to, *inter alia*, heed credible security warnings; maintain adequate patch management policies and procedures; detect alerts in regard to vulnerabilities affecting its systems; properly update and patch third-party software, update software regularly, implement third-party patches when issued, and prioritize patches by the severity of the threat; properly use automated tools to track which versions of software were running and whether updates were available; and implement appropriate procedures to keep security current and address vulnerabilities, including to monitor expert websites and software vendors’ websites regularly for alerts about new vulnerabilities.

141. Only Defendants were in the position to ensure that their information systems, practices, and protocols were sufficient and consistent with industry standards and requirements.

142. Defendants failed to exercise reasonable care to perform these actions. Defendants failed to provide reasonable or adequate information systems and networks and failed to engage in appropriate cybersecurity practices to safeguard their claims processing and revenue cycle services on behalf of Plaintiff and Class Members.

143. Defendants' failure to abide by their duties placed Plaintiffs and Class Members in a worse position than they would have been had Defendants not undertaken such duties because other, more secure means would have been used to process insurance claims and payments for Plaintiff's practice and those of the Class which would have avoided the current disruption and lack of funds flowing to Plaintiff and the Class/

144. Defendants' failure to abide by their duties was wrongful and negligent in light of the foreseeable risks and known threats.

145. Defendants knew or should have known that failure to take appropriate actions to secure its systems increased the risk of harm to Plaintiff and Class Members beyond the risk of harm that existed without the undertaking.

146. As a direct and proximate result of Defendants' negligent undertaking, Plaintiff and the Class Members have suffered and will suffer injury.

COUNT THREE
Negligent Failure to Warn
(On Behalf of Plaintiff and the Classes)

147. Plaintiff restates, re-alleges, and incorporates by reference each and every allegation of the preceding paragraphs of this Complaint as though fully set forth herein.

148. Upon information and belief, Defendants had been aware for a substantial period of time that their cybersecurity systems and networks were inadequate and prone to attack.

149. Defendants knew or should have known of its cybersecurity failures including, but not limited to, failing to heed credible security warnings; failing to maintain adequate patch management policies and procedures; failing to detect alerts in regard to vulnerabilities affecting its systems; failing to properly update and patch third-party software, update software regularly, implement third-party patches when issued, and prioritize patches by the severity of the threat; failing to properly use automated tools to track which versions of software were running and whether updates were available; and failing to implement appropriate procedures to keep security current and address vulnerabilities, including to monitor expert websites and software vendors' websites regularly for alerts about new vulnerabilities.

150. Nevertheless, Defendants failed to warn Plaintiff and Class Members of the known cybersecurity vulnerabilities, failed to effectively remedy the cybersecurity flaws and problems in their systems and networks, failed to warn Plaintiff and Class Members of likely risks caused by Defendants' failure to remedy such cybersecurity flaws, and failed to provide prompt notice to Plaintiff and Class Members that the promised secure information systems had been breached by unauthorized persons during the Cyberattack.

151. As a direct and proximate result of Defendants' negligent failure to warn, Plaintiff and the Class Members have suffered and will suffer injury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all other members of the proposed Class and Subclass, respectfully request that the Court enter judgment in Plaintiff's favor and against Defendants as follows:

A. Declaring, adjudging, and decreeing that this action is a proper class action, and certifying the proposed Class and/or Subclass (“Classes”) pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2), and/or (b)(3), including designating Plaintiff as Class representative and appointing Plaintiff’s counsel as Class Counsel;

B. Awarding Plaintiff and the Classes appropriate monetary relief, including actual damages; statutory damages; consequential damages; punitive damages; exemplary damages; nominal damages; restitution; and disgorgement of all earnings, interest, profits, compensation, and benefits received as a result of their unlawful acts, omissions, and practices;

C. Awarding Plaintiff and the Class and Subclass equitable, injunctive, and declaratory relief as may be appropriate to protect the interests of Plaintiff and Class Members, including but not limited to an Order enjoining Defendants from engaging in the wrongful and unlawful conduct complained of herein;

D. Compelling Defendants to pay the costs associated with notification of Class Members about the judgment and administration of claims;

E. Awarding Plaintiff and the Classes pre-judgment and post-judgment interest to the maximum extent allowable;

F. Awarding Plaintiff and the Classes reasonable attorneys’ fees, costs, and expenses; and

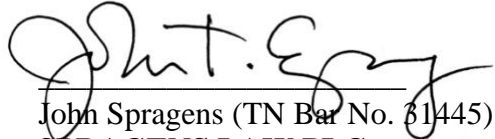
G. Awarding Plaintiff and the Classes such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of the Class and/or Subclass, hereby demands a trial by jury of all issues in this Complaint so triable.

Dated: March 21, 2024

Respectfully submitted,



John Spragens (TN Bar No. 31445)

SPRAGENS LAW PLC

311 22nd Ave. No.

Nashville, TN 37203

Telephone: (615) 983-8900

Facsimile: (615) 682-8533

john@spragenslaw.com

Jennifer R. Scullion*

Christopher L. Ayers*

Justin M. Smigelsky*

Nigel Halliday**

SEEGER WEISS LLP

55 Challenger Road, 6th Floor

Ridgefield Park, New Jersey 07660

Telephone: (973) 639-9100

Facsimile: (973) 639-9393

jscullion@seegerweiss.com

cayers@seegerweiss.com

jsmigelsky@seegerweiss.com

nhalliday@seegerweiss.com

Attorneys for Plaintiff and the Proposed Classes

**Pro Hac Vice* forthcoming

*** Tennessee Bar. Application for Admission to Middle District of Tennessee forthcoming*